Cyber Threat Intelligence and Incident Response Report

Incident ID: 240311_PTDreport_01
Report Author: Brittany Powell
Report Date: 3/12/2024
VPC: 02923045326b5935e

INCIDENT SEVERITY

HIGH	MEDIUM	LOW
x		

SUMMARY

An attacker, primarily using the IP address 10.0.0.176, conducted a series of cyber attacks against multiple targets within the organization, including Accounting 1, Accounting 2, Risk Analyst 1, CFO, Metasploitable, Data Analytics, and Web App systems. These attacks involved brute force attempts on SSH and RDP services, port scans to identify vulnerabilities, and the creation of a malicious webpage.

MITRE ATTACK

1. Reconnaissance [TA0043]

- *T1595: Active Scanning: The attacker performed port scans against various systems (e.g., 10.0.0.176 performing port scans) to identify open ports and services, which is indicative of active scanning.*

2. Resource Development [TA0042]

- ***Not explicitly mentioned, but attackers might have developed or acquired tools and infrastructure (e.g., the IP 10.0.0.176) to support their attack.***

3. Initial Access [TA0001]

- *T1133: External Remote Services: Attempts to access systems through RDP (e.g., 10.0.0.176 attempting RDP through brute force) align with this technique, where attackers target external remote services to gain initial access.*

4. Execution [TA0002]

- ***Not directly mentioned, but executing scripts or commands would be necessary for subsequent stages of the attack.***

5. Persistence [TA0003]

- *T1547: Boot or Logon Autostart Execution: By modifying system settings and user accounts, attackers could create a method for maintaining persistence within compromised systems.*

6. Privilege Escalation [TA0004]

- ***Not explicitly described, but attackers may have attempted to gain higher-level privileges through brute force attacks or by exploiting system vulnerabilities.***

7. Defense Evasion [TA0005]

- *T1027: Obfuscated Files or Information: If attackers introduced malicious executables and DLLs, they might have used obfuscation techniques to evade*

detection.

8. Credential Access [TA0006]

- *T1110: Brute Force: The use of brute force attacks to guess passwords or find valid usernames directly corresponds to this technique.*

9. Discovery [TA0007]

- *T1087: Account Discovery: By gaining access through valid usernames or managing user accounts on the local machine, attackers were likely engaging in account discovery.*

10. Lateral Movement [TA0008]

- *T1021: Remote Services: The use of RDP and SSH by attackers to access other machines in the network indicates lateral movement through remote services.*

11. Collection [TA0009]

- ***Attackers may have collected sensitive information from compromised systems.***

12. Command and Control [TA0011]

- ***The consistent use of IP 10.0.0.176 indicateS it was part of a command and control infrastructure.***

.

14. Impact [TA0040]

- *T1485: Data Destruction: If malicious executables and DLLs introduced by attackers led to unauthorized changes, there might be an impact on the integrity of the data and systems.*

Impact Analysis

Systems and Data:

- *Unauthorized access to systems could lead to the compromise of sensitive data, including financial records, personal information, and intellectual property.*
- *Introduction of malicious executables and DLLs raises the risk of malware infection, potentially leading to data loss or theft.*

Business Operations:

- *Disruption of critical operations due to system compromise could result in significant downtime and financial losses.*
- *Unauthorized changes to system configurations and user accounts may undermine the integrity of business processes.*

Users:

- *Employees and clients could be exposed to increased security risks, including identity theft and fraud, due to potential data breaches.*

Affected Systems/Assets

- *Accounting Systems: 10.0.0.126 and 10.0.0.197, targeted for unauthorized access and data manipulation.*
- *Risk Analyst and CFO Systems: 10.0.0.74 and 10.0.0.206, subjected to RDP brute force attacks, with potential unauthorized changes to system settings.*
- *Metasploitable System: 10.0.0.82, where a malicious file was discovered.*
- *Data Analytics System: Server-BOB (10.0.0.123), compromised via SSH brute force attack, leading to unauthorized access.*
- *Web Application: 10.0.0.175, targeted with SSH brute force attacks and used to host a malicious webpage.*

TIMELINE

Data Analytics Server-BOB 10.0.0.123

INCIDENT TIMELINE

03/11/24 1600	Brute Force Attack SSH from IP 10.0.0.176
03/11/24 1700	The change occurred when the brute force had access to valid usernames.
03/11/24 1806	Bad actor gained access through User: Peter
03/12/24 0905	Nessus.org on 3/12. Status=203/EXEC. Alerted about a problem executing the binary file.
03/12/24 0958	Brute force activity happening in 10.0.0.123 and 10.0.0.126

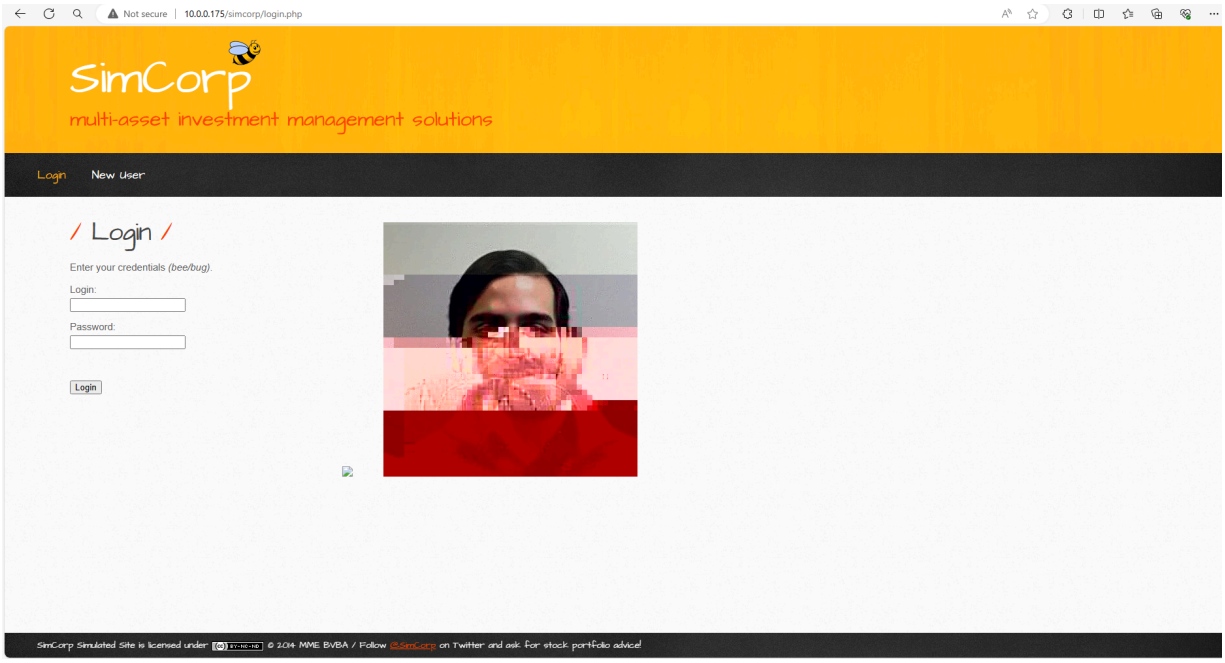
Accounting 2 10.0.0.197

INCIDENT TIMELINE

03/11/24 20:20	Bad actor brute force attempt.
03/12/24 1640 HRS	10.0.0.176 is performing port scans.
03/12/24 1640 HRS	10.0.0.176 is attempting to RDP through brute force.

Web App
10.0.0.175

03/11/23 22:35	**Bad actor created a webpage: http://10.0.0.175**



Accounting 1
10.0.0.126

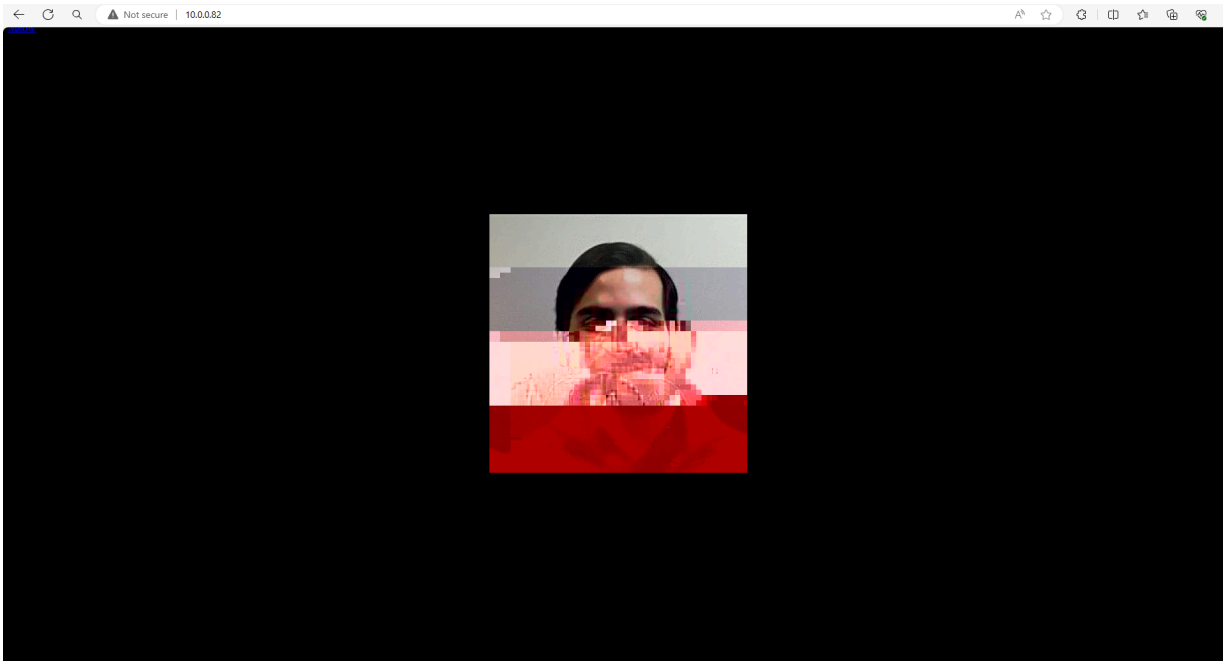
INCIDENT TIMELINE

03/12/24 0958 HRS	Brute force activity happening in 10.0.0.123 and 10.0.0.126
03/12/24 1519 HRS	10.0.0.176 is performing port scans against
03/12/24 1637 HRS	10.0.0.176 attempted to RDP through brute force

Metasploitable
10.0.0.82

INCIDENT TIMELINE

3/12/24 1110 HRS	Malicious file found. http://10.0.0.82



CFO
10.0.0.206

INCIDENT TIMELINE

03/13/24 1908 HRS	10.0.0.176 attempted to RDP through brute force.
03/13/24 1908	Bad actor attempted to access other machines in the network via SSH, and managed user accounts on the local machine.

Risk Analyst 1
10.0.0.74
Incident Type: RDP Brute Force Attack
Target Instance: 10.0.0.74
Source Instance: i-056ee78922f134039

INCIDENT TIMELINE

03/12/24 1952 HRS	10.0.0.176 attempted to RDP through brute force.
03/12/2024 1955 HRS	***security issue where an unauthorized person (bad actor) has gained remote access to a system and is making unauthorized changes, such as modifying Remote Desktop Protocol (RDP) settings, camera and audio settings, and introducing potentially malicious executables and DLLs (Dynamic Link Libraries). This situation is critical and needs immediate attention to prevent further damage or data breach. Here's a step-by-step approach to address the issue.***